ENHANCED HYBRID ACCESS ADMINISTRATION MODEL OF PRIVILEGED ACCESS ADMINISTRATION WITH IDENTITY ACCESS ADMINISTRATION TO ADVANCE THE USER'S PROTECTION PROCEDURES IN ONLINE CIRCUMSTANCES

K.R.SUMATHI[1], Dr.A.ARULJOTHI[2]

[1]Research Scholar, Department of Computer Science, Gobi Arts & Science College,
Gobichettipalayam, Tamil Nadu , India.
[2]Associate Professor, Department of Computer Science,
Gobi Arts & Science College, Gobichettipalayam,
Tamil Nadu , India.

sumathi228@gmail.com[1]
tamil.aruljothi@gmail.com[2]

Abstract

Securing access to vital information systems is crucial in the age of digital transformation. The changing functions of Privileged Access Management (PAM) with Identity and Access Management (IAM) in corporate cyber security frameworks are examined in this study. While PAM adds extra security layers for privileged accounts that are more likely to be hacked, IAM serves as the framework for managing digital identities and regulating user access across business resources. This paper examines the integration and unique features of IAM and PAM systems through a comparative analysis, highlighting how well they work together to mitigate both internal and external risks. In order to assess best practices, implementation difficulties, and the efficacy of unified Hybrid PAM-IAM methods in boosting compliance, decreasing the attack surface, and increasing operational efficiency, the study uses survey data and case studies. The results highlight the necessity of a layered access security architecture and support role-based access restrictions, least privilege enforcement, and ongoing monitoring as fundamental security measures for contemporary digital settings..

Keywords: Identity Access Administration, Cyber Safety Measures, Privileged Access Administration, Risk Evaluation, Network Safety Measures.

1. Introduction

Information system safety measures is more important than ever in the hyper connected, digitalized world of today. From ransomware attacks and insider threats to nation-state espionage, organizations in every industry are facing an unprecedented increase in cyber risks. Managing access to digital resources has become more difficult as cloud services, remote work settings, and third-party connections have proliferated. In light of this, Privileged Access Management (PAM) along with Identity and Access Management (IAM) have become essential clarifications for guaranteeing regulated, auditable, and safe access to corporate resources.

IAM is a complete framework that controls user access to resources inside an IT environment and manages digital identities. It contains measures and tools that assurance the suitable people have admission to the suitable possessions for the suitable reasons at the suitable times. IAM encompasses fundamental operations including governance, user provisioning, de-provisioning, authorization, and authentication. Alongside trends like cloud adoption, mobile device usage, and the growing decentralization of IT infrastructures, IAM's significance has increased.

PAM, on the other hand, is especially concerned with managing and keeping an eye on access to accounts with higher levels of power, such application managers, network engineers, and system administrators. Malicious actors find these accounts appealing because they have extensive control over data, security rules, and system configurations. Compared to a breach involving a standard user account, a successful assault on a privileged account has the potential to inflict far more harm. The intersection of IAM and PAM is increasingly seen as a crucial component of enterprise security architecture, especially as organizations pursue a Zero Trust model—a security framework that assumes no actor, system, or network is inherently trusted. PAM solutions are therefore made to enforce stringent controls, including credential vaulting, session supervising, time-limited admission, and just-in-time dispensation elevation. IAM offers the general framework for identity lifecycle management throughout an organization, while PAM adds an extra, more focused layer of control for high-risk access scenarios.

According to the problem statement, many firms still see breaches caused by compromised credentials or misuse of privileged access, even though there has been a significant investment in cyber security systems. Over 80% of security breaches, according to industry studies, include credentials that have been stolen or misused, frequently as a result of inadequate identity and privilege controls. IAM systems offer a solid foundation for user identity management, but they frequently fall short in terms of granularity and monitoring capabilities needed to protect privileged access. On the other hand, centralized identity intelligence and policy enforcement systems might not be advantageous when PAM techniques are used alone.

This study's scope acknowledges the trend toward hybrid architectures in contemporary IT landscapes, encompassing both on-premises and cloud-based settings. It takes into account a wide range of use cases, from small and medium-sized businesses to big, regulated areas like government, healthcare, and finance. The study ensures theoretical accuracy and practical relevance by drawing on industry data, scholarly literature, and standards from organizations like NIST, ISO, and CISA.

Its ability to assist enterprises in shifting from reactive, compartmentalized security postures to proactive, comprehensive identity-based security frameworks is what makes this research significant. Organizations must put in place access restrictions that are not only technically sound but also flexible enough to adjust to shifting business and regulatory needs as threats and attackers become more complex.

After this introduction, the paper will provide a thorough literature analysis that charts the development of IAM and PAM technologies, highlighting new developments such as cloud-native access management and AI-driven identity analytics. The methods for evaluating IAM and PAM maturity, comparison analyses, and performance indicators will be covered in the following sections. Recommendations, constraints, and future prospects for practice and research will be discussed in the paper's conclusion.

2. Review of related literature

Indu.et.al. Cloud computing is one of the complex structures that facilitate requested services by coalescing a multiplicity of associated gadgets. Different types of flexible disseminated systems with a extensive assortment of connectivity along with consumption make up the structural design of online computing. Because cloud networks provide advantages including cost-effectiveness, scalability, dependability, and flexibility, businesses are embracing them quickly. Online associations are susceptible to several types of association assaults and seclusion concerns, despite the fact that the main benefits of cloud computing are encouraging realities. Identities with admittance control mechanisms are compulsory due to online situation features like multiple-tenancy along with intermediary managed communications.

Plentiful academics with business professionals have addressed the problems of safe access to online resources. The challenges associated with cloud authentication, access control, security, and services are reviewed in this article, along with suggested solutions. Identity along with admission management, safety measures concerns, and cloud services are all addressed in this thorough comparison of the current methods from the viewpoints of cloud service providers and users.

Saloni.et.al.IAM is deposits of procedures, practices, along with resources that assist companies organize customer admittance to private company data along with digital personas. By giving customers defined positions and guaranteeing they have the accurate amount of admission to corporation possessions and associations, IAM enhances safety measures and customer understanding, facilitates healthier company results, and augments the feasibility of transportable and isolated operational as well as online embracing. The IAM service only supports a single form of resource-based strategy, referred to as a responsibility confidence strategy furthermore associated to an IAM responsibility.

Resource-based policies are made possible by an IAM responsibility, which provides as mutually distinctiveness and a source. As a result, an IAM role has to have both an identity-based policy and a trust policy. The individuality and admission administration scheme forms the basis of the program. Making sure the proper public has appropriate admission to the relevant possessions is a basic and crucial cyber security capability. IAM comprises four domains: Advantaged Access Administration, third-party Distinctiveness Supremacy and Management, information supremacy and fortification, and IAAA, which stands for individuality, substantiation, endorsement, and secretarial. This article explains how IAAA functions in an online environment and covers the ideas of identity, authentication, authorization, and accounting.

Hardik.et.al. Researchers from all over the world are constantly adding new features and capabilities to the still-emerging and quickly changing concept of cloud computing. Large-scale distributed computing technology is the foundation of cloud computing. In actuality, it is a continuation of grid computing, and the new technologies of the future—distributed computing and parallel computing—will only connect to the cloud to access the processing power they require. Security as online services or security offered via the online moderately than on premise safety measures resolutions, are the major prominence of the Security-as-a-Service conception.

The regions of spotlight for Identity and Access Administration and Privilege and Access Management include audits, secure access, zero trust privileged individuality, endorsement, along with administration. Its major apprehension are confirming the entity's identification and surrendering the suitable degree of admittance to online-sheltered possessions. Every business, government organization, and higher education institution aspires to have a secure, adaptable, and agile IT infrastructure, and identity management is the cornerstone of true digital transformation.

Almost every significant application and procedure in the majority of businesses will make use of the creation and dissemination of IDs. In the end, individuality should be a effectiveness; it should be simple to recognize people, programs, with objects furthermore utilize them as required while adhering to appropriate security measures that prioritize privacy. Another crucial aspect of how businesses deal directly with customers and trading partners is identity management. The user may take use of all the benefits that Security-as-a-service has to offer when IAM and PAM are deployed as cloud services.

The author has put a proof-of-concept (POC) for SaaS into practice. In order to give cloud users safe access, the pertinent standards and technologies are also put into practice and addressed. The Identity and Access Administration, Dispensation and Access Administration as a examine structure, Tools/Knowledge, and accomplishment frameworks are proposed by the author in this study.

Surendra.et.al. The cyber security environment has been profoundly influenced by the quick development of artificial intelligence, especially in the areas of uniqueness supremacy and management, privileged access administration, and identity and access management. These technologies are essential for managing and keeping an eye on who has access to private information and systems inside businesses. By adding mechanization, extrapolative analytics, and concurrent administrative, artificial intelligence (AI) improves conventional IAM, PAM, and IGA systems. This enables businesses to proactively manage access controls, identify risks, and guarantee regulatory compliance. The growth and importance of AI in improving cyber security across several sectors are examined in this essay by the author, who highlights important advantages such enhanced hazard recognition, less person mistake, along with expedited conformity procedures.

It looks at how artificial intelligence changes conventional static security measures into intelligent, adaptable systems that can react quickly to new threats. The author also talks about difficulties including the requirement for specialized skills, integration difficulties, and data protection issues. Looking ahead, there are a lot of intriguing potential for AI in IAM, PAM, and IGA, such as improved predictive security, autonomous access management, and deeper connections with blockchain technology. These developments could help firms better defend against increasingly complex cyber threats by fortifying their security postures.

Jessie.et.al.One of the majority important elements of contemporary online safety measures frameworks is Identity and Access Administration. Strong access controls, authentication procedures, and identity governance are essential as more and more tasks are moved to the cloud by enterprises. The author examines IAM's function in protecting cloud workloads, going over its main ideas, procedures, and recommended practices. In order to reduce security threats, the study emphasizes the significance of role-based admission organize, multi-factor substantiation, furthermore ongoing monitoring. Additionally, this research looks at a number of IAM implementation issues and solutions, with a focus on industry standards and regulatory framework compliance.

The results highlight how important IAM is for lowering unwanted access, stopping data breaches, and guaranteeing safe cloud environments. Since cloud computing is now the foundation of contemporary business operations, IAM makes guarantee that critical resources are only accessible by authorized people and devices. In order to improve cloud security, this research explores sophisticated IAM techniques such identity federation, Just-in-Time (JIT) access control, and Zero Trust Architecture (ZTA). It also investigates how automated provisioning and AI-driven identity analytics might lessen security flaws.

In order to show how strong IAM rules may reduce insider threats, account takeovers, and privilege escalations, the research focuses on important industrial use cases. By offering firms practical insights to adopt complete security measures that are in line with changing cyber threats and compliance norms, this research adds to the expanding body of knowledge on IAM.

3. Methodology

The efficacy of a unified Identity and Access Administration furthermore Privileged Access Administration framework is assessed in this study using a hybrid research methodology that combines qualitative and quantitative techniques. The goal of the exploratory study is to pinpoint the best practices, installation difficulties, and performance enhancements related to hybrid PAM-IAM systems in business settings.

PAM is a collection of protocols, rules, and resources that assist companies in managing their online identities. PAM systems are specifically designed to manage and secure administrators and users with higher permissions. IAM gives businesses the ability to verify and authorize all of their users' internal employees, external clients, partners, and vendors transversely their entire assault facade and technologies, including Active Directory. The proposed approach combined the PAM and IAM to hide some special needs in the particular environmental applications.

The pattern of a user's activity is examined to determine whether they are being created. Verifying the user-name and secret word is a widespread technique for description login and agency substantiation. Data about the customer may be gleaned from how the description is utilized. It will be taken into consideration if a customer's login location differs from the standard. A customer's arrangement and information admittance position are checked to ascertain their legitimacy.

The elimination of a folder devoid of departure any trace, which is forbidden by some criteria, is an example of an anomalous event. The customer is allowable to clutch out their vital duties after their organization satisfies the required safety measures standards. Customer logins and information admittance from unregistered gadgets are also measured. Using preconditions for recognition authentication and avoiding a user's susceptible behavior to stop unwanted activity.

To determine whether a customer is being created, the outline of their activity is compared. One admired practice for explanation login and agency substantiation is the authentication of the username along with password. The approach the version is utilized might expose data about the customer. In the event that a customer's login position deviates from the model, it will be measured. To establish a customer's identity, their organization and information admission position are demonstrated. One instance of an unusual event is the deletion of a file exclusive of departure an outline, which is proscribed by a number of criterions.

Once their organization meets the compulsory safety measures criteria, the customer is allowable to do their vital responsibilities. Furthermore taken into account are customer logins and information admittance from unregistered gadgets. Using preconditions and identification verification to prevent unauthorized activity and a user's susceptible behavior.

Characteristics and Benefits of the Hybrid Model (HM):

- **Least Privilege Principle:** Only allow access to what is required. Not every user needs complete access privileges, and not every member of the kingdom needs access to the royal treasury.
- **Secure Shared Accounts:** Shared accounts may provide a risk. PAM uses session monitoring and automated password resets to make sure that shared access is strictly regulated.

- **Robust Authentication:** The gatekeeper is multi-factor authentication (MFA), which requires more information than simply a password. Tokens, smart cards, or biometrics provide an additional degree of security.
- **Continuous Monitoring and Auditing:** Being alert is essential. PAM monitors everything, recording every action that takes place in the realm. Frequent audits guarantee that any illegal access is promptly addressed.
- **Session Recording and Playback:** Knowing the order of events in a breach is essential. All sessions are recorded and archived by PAM, which also offers forensic analytical playback capabilities.
- **Automated Password Management:** Human mistake is unavoidable, particularly when it comes to passwords. By automating password updates, PAM lowers the possibility of credentials being compromised.
- **Regulatory Compliance:** By ensuring compliance with legal requirements, HM protects the kingdom against legal action.
- **Operational Efficiency:** HM improves efficiency by streamlining access and automating procedures, which enables the kingdom to run smoothly.
- **Threat Mitigation:** HM reduces the chance of breaches by acting as a proactive barrier against possible threats by restricting access and keeping an eye on activity.
- **Enhanced Security:** HM aids in limiting access to certain resources to approved systems or users. This considerably lowers the possibility of insider threats, data breaches, and illegal access.
- **Compliance and Governance**: HM makes it easier to comply with legal mandates and industry norms. By monitoring activity, generating audit trails, and enforcing access regulations, it assists enterprises in proving compliance.
- **Improved Productivity:** Simplifying the on-boarding and off-boarding procedures for users guarantees that they are promptly given access to the system resources required for their work and that their access is terminated as soon as they are no longer required. Overall productivity is increased as a result.
- **Efficient User Provisioning and Deprovisioning:** Automated provisioning along with deprovisioning speeds up user on-boarding and off-boarding, ensures consistency, and lowers human error. In bigger firms with regular staff changes, this is especially crucial.
- **Reduced Security Risks:** Strong authentication and the least privilege principle are two examples of proper HM practices that help create a more secure environment. HM assists companies in reducing the dangers of illegal access and compromised credentials.
- **Cost Savings:** By ensuring that users only have the required access rights, HM assists companies in allocating resources as efficiently as possible. This lowers the possibility of over provisioning and may result in lower operating and licensing costs.
- **Centralized Access Control:** For access control and administration across several systems and apps, HM offers centralization. This unified control makes security policy enforcement easier and improves visibility.
- **Enhanced User Experience:** By tumbling the numeral of times customers must record in, HM systems' Single Sign-On (SSO) features enhance the user experience. User happiness rises as a result of this convenience.

- **Increased Accountability:** By recording user actions and access events, HM systems generate an audit trail. In the event of a security breach, this responsibility helps with forensic investigation and deters harmful activity.
- **Adaptability to Change:** HM frameworks are made to adjust to organizational changes, including adjustments in technology, system integrations, and staff roles. This adaptability promotes future-proofing and scalability.
- **Protection against Insider Threats:** HM lowers the danger of insider attacks by assisting enterprises in managing and monitoring user access. Organizations can identify and address questionable activity by monitoring and managing user actions.
- **Improved Password Management:** HM systems frequently provide tools for enabling self-service password resets, simplifying safe storage, and enforcing strict password standards. This helps create a stronger authentication system.
- **Strategic Decision-Making:** Organizations are empowered to make well-informed decisions on security protocols, compliance tactics, and access policies by having access to the comprehensive reports and analytics that HM systems give.
- **Support for Cloud and Mobile Environments:** HM systems offer a unified method of maintaining identities in contemporary, dispersed contexts by integrating with cloud services and supporting mobile devices.

4. Results and Discussions

Table.01.Evaluation of different information security components with percentage

S. No.	Information security component	Mansour et. al	ISO/ IEC	Eloff et. al	Veiga et. al.	Tudor et. al	Proposed HM 1	Proposed HM 2
1.	Governance	Y	X	X	X	X	Y	Y
2.	Security strategy	Y	Y	X	Y	X	Y	Y
3.	Leadership	Y	Y	Y	Y	Y	Y	Y
4.	Security organization	Y	Y	Y	Y	Y	Y	Y
5.	Policies, standards, and guidelines	Y	Y	Y	Y	Y	Y	Y
6.	Measurement metrics & ROI	Y	X	Y	Y	X	Y	Y
7.	Compliance and monitoring	Y	Y	Y	Y	Y	Y	Y
8.	User management	Y	Y	X	Y	X	Y	Y
9.	Training & awareness	Y	Y	X	Y	Y	Y	Y
10.	Ethics	Y	Y	Y	X	X	Y	Y
11.	Privacy	Y	Y	X	Y	X	Y	Y
12.	Trust	Y	Y	X	X	Y	Y	Y
13.	Certification	X	X	Y	X	X	X	X
14.	Best practice	X	Y	Y	Y	Y	Y	Y
15.	Asset management	Y	Y	Y	X	X	Y	Y

16.	Physical and environmental security	X	Y	Y	Y	Y	X	X
17.	Technical operations	Y	Y	Y	Y	Y	Y	Y
18.	System acquisition, development and maintenance policy	Y	Y	Y	Y	X	Y	Y
19.	Incident management plan	Y	Y	X	Y	X	Y	Y
20.	Business Continuity plan	Y	Y	X	Y	Y	Y	Y
21.	Disaster recovery plan	Y	X	X	Y	Y	Y	Y
22.	Risk assessment process and plan	Y	Y	Y	Y	Y	Y	Y
23.	Customized Policy Plan	X	X	X	X	X	X	Y
24.	Equipped Effectiveness	X	X	X	X	X	X	Y
25.	Adaptability to transform	X	X	X	X	X	X	Y
Number of components with Y (Yes)		19	18	13	17	12	20	23
Number of components Y (Yes) %		76	72	52	68	48	80	92
Number of components with N (No)		06	07	12	08	13	05	02
Number of components N (No) %		24	28	48	32	52	20	08

**Y = Yes, X = No*

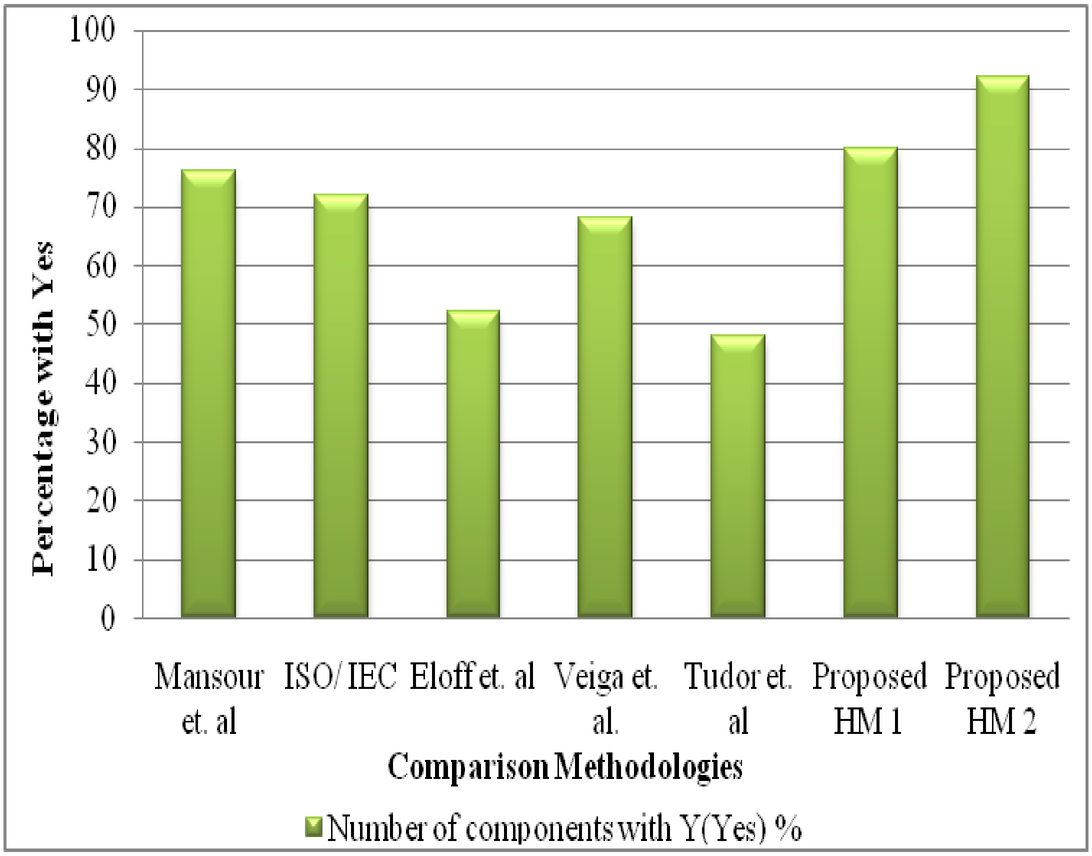

Figure.01.Comparison of different information security components with Positive percentage

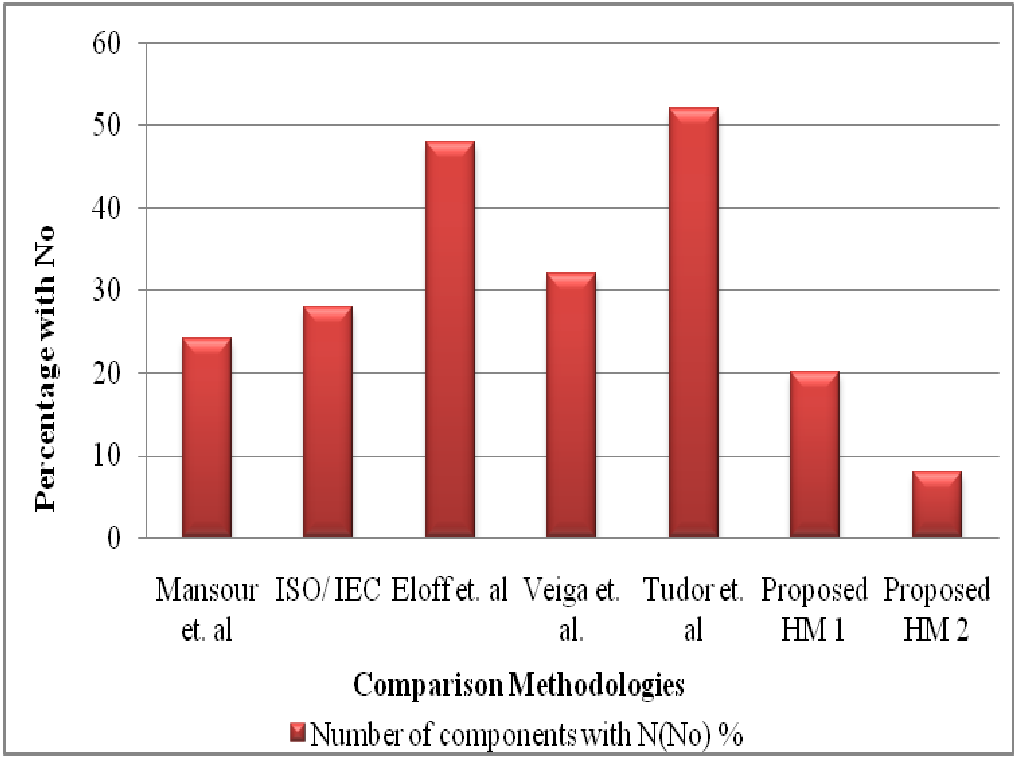

Figure.02.Comparison of different information security components with Negative percentage

Table 01 shows the predicted concept's efficacy in comparison to the available data safety measures system. The percentages that were good and negative between the departing procedures were displayed in Figures 01 and 02.

5. Conclusion

It is more important than ever to secure access to vital systems and data in the increasingly complicated and digitalized IT ecosystem of today. This study emphasizes how important Identity and Access Management (IAM) and Privileged Access Management (PAM) are to creating a thorough access security plan. PAM concentrates on the supervision and defense of high-risk privileged accounts, whereas IAM controls the identities and access privileges of every user. In order to minimize the attack surface, stop internal and external threats, and maintain regulatory compliance, their integration is not only advantageous but also necessary.

According to the results, companies that use a combined IAM-PAM strategy which is founded on ideas like role-based access management, least privilege, and continuous monitoring achieve greater operational security and efficiency. However, thorough preparation, organizational dedication, and an awareness of both technology and human issues are necessary for successful implementation. In the end, our study confirms that IAM and PAM are interconnected parts of contemporary, robust cyber security architecture rather than stand-alone solutions.

Building trust in business settings and facilitating safe digital change depend heavily on their synergy. Access control and security risk reduction are unquestionably improved by the hybrid deployment of IAM and PAM. Businesses are better equipped to satisfy compliance requirements, protect against internal threats, and enable dynamic, cloud-based operations when they see these technologies as complimentary rather than separate components.

References

1. Moustafa Mamdouh, Ali Ismail Awad, Ashraf A.M. Khalaf , Hesham F.A. Hamed, “Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions”, Computer and Security, Vol.111, 2021, pp. 01 – 24.
2. Chetanpal Singh, Jatinder Warraich , Rahul Thakkar, “IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations”, European Journal of Engineering and Technology Research, Vol.08, No.04, August 2023, pp. 30 – 39.
3. Kaushik Reddy Muppa, “Analysis on the Role of Artificial Intelligence and Identity and Access Management (IAM) in Cyber Security”, International Journal of Artificial Intelligence Research and Development, Vol.02, No.01, January-June 2024, pp. 113 – 122.
4. Siddhesh Bhargude, “Privileged Access Management: Ensuring Security and Accountability”, International Journal of Advanced Research in Science, Communication and Technology, Vol.03, No.01, July 2023, pp. 647 – 651.
5. Diana Gudu, Marcus Hardt, Lukas Brocke, Gabriel Zachmann, “Enabling Secure Shell Access with OpenID Connect”, Computing and Software for Big Science, Vol.09, No.5, 2025, pp. 01 – 14.
6. Deepa Ajish, “The signifcance of artifcial intelligence in zero trust technologies: a comprehensive review”, Journal of Electrical Systems and Information Technology, Vol.11, No.30, 2024, pp. 01 - 23.

7. Naveen Pratiksha, Prof. S. G. Raghavendra Prasad, Dr. Jitendranath Mungara, “Identity and Access Management”, International Journal of Engineering Science and Computing, Vol.07, No.05, May 2017, pp. 11907 – 11912.
8. Reddy, C. S., Yookesh, T. L., & Kumar, E. B. (2022). A study on convergence analysis of Runge-Kutta Fehlberg method to solve fuzzy delay differential equations. Journal of Algebraic Statistics, 13(2), 2832-2838.
9. M. Liu, and X. Wang, “Safeness Discussions on TRBAC and GTRBAC Model and an Improved Temporal Role - Based Access Control Mode”, International Journal of Security and Its Applications, 2015, vol.9, no.8, pp. 23 – 34.
10. B. Hicks, S. Rueda, D. King, T. Moyer, J. Schiffman, Y. Sreenivasan, P. McDaniel, and T. Jaeger, “An architecture for enforcing end-to- end access control over web applications,” 15th ACM Symposium on Access Control Models and Technologies, 2010, pp. 163 – 172.
11. S. Hasani, and N. Modiri, “Criteria Specifications for the Comparison and Evaluation of Access Control Models,” International Journal of Computer Network and Information Security (IJCNIS), 2013, vol.5, no.5, pp. 19 – 29.
12. I. Indu, P.M. Rubesh Anand, Vidhyacharan Bhaskar, “Identity and access management in cloud environment: Mechanisms and challenges”, Engineering Science and Technology, an International Journal, Vol.21, 2018, pp. 574 – 588.
13. Hardik Varma, “Identity Access Management (IAM), Privilege Access Management (PAM) & Security Operation Center (SOC)”, International Journal for Research in Applied Science & Engineering Technology, Vol.09, No.11, November 2021, pp. 1460 – 1466.
14. Saloni Kumari, “Identity and access management: Elevating security and efficiency: Unveiling the crucial aspects of identity and access management”, International Journal of Engineering & Technology, Vol.12, No.01, 2023, pp. 11 – 14.
15. Surendra Vitla, “Leveraging AI-Enhanced IAM, PAM, and IGA for Cybersecurity: A Cross-Industry Approach to Reducing Cyber, Journal of Information Systems Engineering and Management, Vol.10, No.16, 2025, pp. 70 – 91.
16. Jessie Anderson, “The Role of Identity and Access Management (IAM) in Securing Cloud Workloads”, December 2022, pp. 01 – 13.
17. Abinesan S, and E. Boopathi Kumar, “Multi-Factor Authentication for Biometric Verification Using Facial Recognition”, International Journal of Innovative Research in Computer Science and Technology (IJIRCST), Volume-13, Issue-3, May 2025 https:/doi.org/10.55524/ijircst.2025.13.3.1, Pages 1-7
18. Prakash, G., P. Logapriya, and A. Sowmiya. "Smart Parking System Using Arduino and Sensors." *NATURALISTA CAMPANO* 28 (2024): 2903-2911.